Mighty Guides®

Sponsored by

Trustwave®

7 Experts on Security Maturity

Best Practices to Improve a Company's Security Posture

INTRODUCTION: SECURITY MATURITY

When it comes to cybersecurity, how do you know your organization is doing enough to protect itself? One way is to fall victim to an attack and decide after the fact that you weren't doing enough. That works, but there is a better way. You can assess the maturity of your security practice and then decide if it is appropriate for your business.

But how do you think about, measure, improve and communicate the state of your security maturity? With threats coming from every direction and non-technical people, such as business managers, playing a more prominent role in security planning, this is especially challenging. To learn how companies manage their security maturity, and with generous support from Trustwave, we asked seven security experts the following question:

What advice would you give on how to improve the maturity of a business's security practice?

This is an interesting collection of essays because the experts approach the question from the perspectives of their businesses. One expert stresses the importance of starting with your deployment pipeline, while another recommends benchmarking to a security framework. All the experts agree that security maturity must be discussed and measured in a business context, because ultimately it deals with business risk.

I find these essays provide refreshing perspectives on a challenging issue every organization faces today. I hope you agree.

All the best,

David Rogelberg
Publisher, Mighty Guides Inc.

Mighty Guides®

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

FOREWORD: SECURITY MATURITY

Security professionals face mounting pressure to adapt their security program to an evolving threat landscape without inhibiting the mission of their business. From fast growing small- and medium-sized businesses to large global enterprises, communicating with other business leaders about strengths, gaps, and needs is critical to building and sustaining an adaptive cybersecurity program.

Getting to an adaptive cybersecurity program means increasing security maturity: moving from basic reactive security measures like deploying firewalls, to more proactive ones like automated alerts, to finally getting to continuous and pervasive monitoring and visibility of threats. Leveraging security maturity as a transformation tool lets you communicate along the journey to determine where you need to be, based on your risk tolerance, and demonstrate how investments have increased the effectiveness and maturity of your security program.

We created this Mighty Guide so that industry leaders can share with you how their organizations have leveraged security maturity as tool to evolve and mature their cyber capabilities. They provide a range of perspectives on getting people, processes, and technology working in harmony as well as excellent advice on aligning security with risk tolerance and business culture. Transitioning from a reactive, to a proactive and adaptive operation typically follows a consistent approach but each organization brings unique experiences and trials worth sharing as lessons learned.

Regards,
Kory Daniels
Global Managing Partner - Detection, Analytics, and Response Consulting
Trustwave

Trustwave®

Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data, and reduce security risk. Offering a comprehensive portfolio of managed security services, security testing, consulting, technology solutions and cybersecurity education, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.

Trustwave®

There's a New Leader in Cybersecurity

A Leader

2018 Magic Quadrant
for Managed Security Services,
Worldwide

Gartner

Cybercriminals are relentless. So are our security experts, ethical hackers and researchers. Recognized as a leader by the top cybersecurity industry analysts and media outlets, they protect data around the clock for businesses in 96 countries. Transform the way your business manages security with cloud and managed security services from Trustwave.

TABLE OF CONTENTS

DANIEL SCHATZ

Chief Information Security Officer
Perform Group

Daniel Schatz is CISO at Perform Group's London office. Prior to this he led the global Threat and Vulnerability Management program for Thomson Reuters. He is a chartered security professional (CSyP) and a member of the International Systems Security Association (ISSA-UK), and he holds several qualifications including CISSP, CISM, CCSK, CVSE, MCITP-EA, ISO 27001 LA/LI, and MS Information Security and Computer Forensics.

Twitter I LinkedIn

For many organizations, adopting or managing to a security framework provides a proven mechanism to baseline their current security capabilities, set goals, and establish a plan for improving security maturity. Daniel Schatz, chief information security officer (CISO) at Perform Group, agrees, saying, "A maturity baseline is defined by the information-security management system, and my view is that the majority of regulatory and legal requirements are met by a proper implementation of any of those management frameworks." Going through a gap assessment process is a good way to see how your practice stacks up against a security-management framework. "If you're just starting out with a framework, you may not hit all of the controls," Schatz says. "However, as you successfully adopt more controls from any of the frameworks, the maturity of your security program will improve." An added benefit of using a framework is that it establishes a common language for discussing security across the organization.

Schatz notes it's important to look beyond the framework to develop a security program that aligns with business goals and makes investments that improve the practice. Schatz explains his approach. "I try to tie investments into the security strategy, and I try to make sure that the investments that we put into information security are actually contributing to a goal. This is primarily an information security goal, but the goals that I have in my security function always tie to overarching business goals. So I'm not going off on a tangent buying a new solution because I like the fancy dashboard or the graphics." »

> *"As you climb that maturity ladder on any of the frameworks, the maturity of your practice should improve."*

He acknowledges there are sometimes pressures to make investments that might not fit the program. "The reality is there's probably no really bad reason to invest in security. There may be mistimed reasons. If you're under pressure because you had a publicly exposed breach and you need to dosomething, is that the right point in time to invest? Probably a little too late, but better then than not at all." But he emphasizes that it's important to have a strategy that builds a more mature practice for fulfilling the company's security needs. "I'm more focused on consolidating my spend into things that advance my maturity and I know are going to help me stop fighting fires and be more proactive," says Schatz.

Technologies that make a more proactive approach to security possible usually involve tools that automate basic functions such as detecting unusual network activity and initiating responses. "One sign of a reasonably mature security organization is that most of its operational tasks are automated," Schatz says. "It doesn't help me to keep buying the latest machine-learning gadgets if they are not properly tied together. The strategic solution here would be to look at whether a security orchestration and automation solution makes sense."

Aligning to a framework not only helps establish and track the maturity of your security practice, it also helps when talking about it. Information-security frameworks typically break out into categories, and each category is made up of a set of controls, which makes it easier to benchmark and measure »

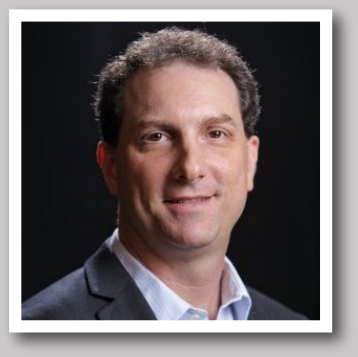
"One sign of a reasonably mature security organization is that most of its operational tasks are automated."

how you have progressed in those categories. Executives will not be so interested in control details, but they will be interested in seeing improvements in the security program. Schatz points out, "Board members are not likely interested in seeing the categories, but they will want to see a consolidated version that addresses things of interest to them like business continuity or approaches to compliance." ■

KEY POINTS

1. Going through a gap assessment process is a good way to see how your practice stacks up against a security-management framework.
2. Having a program that builds toward meeting the company's security needs better enables you to focus on consolidating spending into things that advance maturity and help you to become more proactive.

START WITH A BASELINE AND VALIDATE AS YOU GO



DAVE RUEDGER

Chief Information Security Officer
RMS

Dave Ruedger is an established director of cybersecurity and IT operations with demonstrated success building, deploying, and managing secure IT operations across heterogeneous computing environments. He is a self-directed individual with a proven track record of managing IT infrastructure, operations, business applications, product development, and support, and a leader who motivates individuals to succeed while promoting a collaborative team environment.

LinkedIn

Dave Ruedger, chief information security officer (CISO) at RMS, has had a lot of experience beefing up security practices. "I've worked with organizations that have had a lot of turnover and haven't invested as much as they should. I've also gone into organizations where they are starting from scratch." Based on these experiences, Ruedger recommends three basic activities to build the maturity of a security practice:

1. **Baseline everything.** "You can't fix what you don't know," says Ruedger, "so you have to baseline pretty much everything." This would include your IT assets, existing security tools and resources, and security program goals. He notes there are a number of tools available that help inventory IT assets and security tools, and provide a comprehensive view across an entire security program. He recommends investing in those early on. Additionally, conversations with other executives in your organization can help shape goals that match business needs. Ruedger also notes the important of managing to a security framework. Frameworks help you identify where you have gaps and the gaps to fill to give your resource-constrained organization the most security benefit. Frameworks also provide a common language that helps executives in your organization better understand what security is doing, and it helps you better understand how to support their business requirements. Ruedger suggests, "If you don't have a framework, the first thing is to decide on something that you can map against to build your controls. Even if you're not trying to get a certification, it's a good idea to adhere to something like the CIS Critical Security Controls , for example. They translate very well to all of the frameworks like ISO, »

> *"You can't fix what you don't know, so you have to baseline pretty much everything."*

C5, and SOC2. That will get you to a level of maturity where an outside auditor can come in to attest to the efficacy of your program."

2. **Check to validate your practice.** Ruedger notes that you have to build in checkpoints to validate that you are actually doing what you believe you are doing, and that it's good to get into the habit of regular checks regardless of certification requirements, as a way to periodically assess the state of your program. "This typically means bringing in outside resources to do spontaneous internal audits," he says. "You need that if you're doing any type of certification. It's a good idea to get into that mode of thinking very early on." Once you have a more mature practice, you will need to invest in resources in-house to perform these checks on a regular basis. Ruedger uses both manual and automated checks for this. "I'm really excited about the program we're building where I have people looking at some things from a very manual perspective. They are thought-checking things based on where we find risk. And then we're starting to build automation into some of the processes that we have in place." User management, access controls, and identity management are big areas where organizations quickly expose themselves to risk. As users change roles within an organization, they can accumulate access to information they no longer need and really shouldn't have. Ruedger is implementing an automated spot check that looks at group membership and access controls, and it sends out validation requests to group owners. »

> "If you're not doing regular metrics and reporting, it's very difficult to get buy-in from upper management to support your initiatives."

START WITH A BASELINE AND VALIDATE AS YOU GO

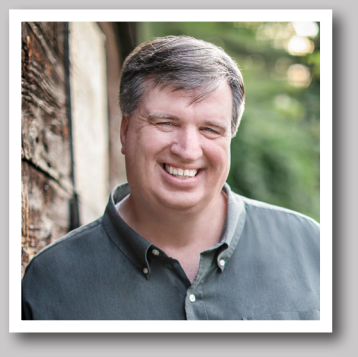
3. **Build meaningful metrics.** Building strong metrics around your practice that non-security folks can understand enables you to see what is happening, measure progress, and have conversations about that with others in your organization. Ruedger says, "If you're not doing regular metrics and reporting, it's very difficult to get buy-in from upper management to support your initiatives." That will make it difficult to improve the maturity of your practice, because the expectation is you're going to be able to support the business and keep the company secure even as threats increase. Which metrics you use depends on the context, but C-level people are most interested in metrics that reflect risk and impact to the business. ■

KEY POINTS

1 You need to perform regular audits to be sure your practice is doing the things you believe it is doing. This will be a mix of both manual and automated checks.

2 Building strong metrics around your security practice enables you to see what is happening and measure progress. C-level people are most interested in metrics that reflect risk and impact to the business.

ALIGNING BUSINESS & SECURITY CULTURE IS CRITICAL



DAVID BILLETER

Chief Information Security Officer
CA Technologies

David Billeter is chief information security officer for CA Technologies, where he is responsible for leading CA's global and diverse information security and IT risk strategy. Previously he led information security for Staples and the InterContinental Hotels Group. Outside of the office, David is an active member in the cyber security industry in the Boston area.

Website I Blog I LinkedIn

To build a more mature security practice, it's essential to build a program where business and security culture align. This means first of all understanding the security culture within the business, and then working to change it if necessary. For instance, is security viewed as an IT technical function, or is weighing cyber risk an integral part of business strategy? Is there a high degree of security awareness in the business, or not so much? David Billeter, chief information security officer (CISO) at CA Technologies, underscores the importance of understanding business culture and business requirements, and identifying how your security program needs to align to those things. "If you're trying to fight the culture, you're going to struggle," he says. "There are going to be times where you will need to influence that business culture, and maybe change it. If you're doing that, you want to make sure you're hitting the right places." This involves focusing on aspects of the culture and practice that will deliver the most security benefit to the business. "You don't want to spend a massive amount of effort for something that isn't important and that's going to be very, very difficult to move the business in that direction," says Billeter. "On the other hand, if something's really important for security, even if you've got to change the business culture, then it's worth it. But you really have to understand the business culture and pick those battles carefully."

In addition to knowing the business culture, you need to make sure you have solid visibility into all of your systems. This includes knowing the people, processes, and technologies you have in place and the whether the results they're achieving are meeting what your business requires now and what you expect requirements will be in the future. Without this information, you can spend a lot of time working on tools and improving processes that totally miss key systems. »

> *"If you're trying to fight the culture, you're going to struggle. You want to align your security maturity with business culture and requirements."*

ALIGNING BUSINESS & SECURITY CULTURE IS CRITICAL

With better visibility and an understanding of security needs in the context of the business culture, you will be ready to start thinking about the processes and technologies you need to update and refine your security practice. Billeter recommends looking for areas to automate security processes at this point. "Automation becomes the glue that holds technologies and processes together," he says. "I think of the automation layer as the operating system for your entire security function. Only after the automation piece is in place and functioning will I get into analytics, like behavioral analytics. You won't get as much out of analytics until you've got the other pieces in place."

There are several reasons why automation plays such a key role in improving security maturity. For one thing, it makes security teams more scalable. Automation also makes tasks repeatable, which not only saves time, but it reduces the possibility of human error. Furthermore, automation makes tasks trackable through logs that can be reviewed. All of these capabilities are characteristic of a more mature security practice.

Achieving higher levels of security maturity requires a thoughtful process. It's important to make smarter decisions about security priorities and investments, because there are lots of things that will become distractions to a security program. You might turn on the news tomorrow and there will be a new unexpected threat that didn't exist the day before. "Then you may have to adjust," says Billeter. "When ransomware really took off, a lot of people had to change their strategy."

> "Automation becomes the glue that holds technologies and processes together."

ALIGNING BUSINESS & SECURITY CULTURE IS CRITICAL

The overall strategy of aligning your security program to your business culture and requirements helps you stay focused even in the face of distractions. That's important because it takes time to build a more mature security program. Belliter says, "Having a strategy is key because you don't have an unlimited amount of time. If you're going to do proof of concepts, that's going to take time and effort from your team. Make sure you're doing ones that will be valuable to you, and not just the latest thing that's come up." ■

KEY POINTS

1. When building a security practice, focus on aspects of the culture and practice that will deliver the most security benefit to the business. If this involves influencing business culture, pick your battles carefully.
2. A thoughtful process helps make smarter decisions about security priorities and investments, and that's important because there are lots of things that become distractions to a security program.

SECURITY MATURITY MUST BE VIEWED IN A BUSINESS CONTEXT

DEEPAK PALAKUNNATH KUNNENKERI

Information Security & Audit Manager (RISO)
Fuji Xerox Asia PAcific Pte Ltd.

Deepak Palakunnath Kunnenkeri is an information-security evangelist with more than 15 years of expertise in cybersecurity, IT audits, regulatory compliance, and cloud and robotic security. He believes staying conversant and combating cyber threats is the key to surviving the digital world. Drawing on his business acumen, he empowers the organization to turn information risk into a corporate advantage and achieve robust digital hygiene.

Twitter I LinkedIn

Improving security maturity begins with understanding the business and its risk tolerance, its critical assets, and threats to those assets. Only then can you evaluate your existing security practice and advance its maturity. "You have to go to the ground level and understand from the business operation what they are expecting from security," stresses Deepak Palakunnath Kunnenkeri, information security and audit manager for Xerox Asia Pacific. "You have to look at the core business, understand the business assets, talk to senior management, and understand what the business operation is all about."

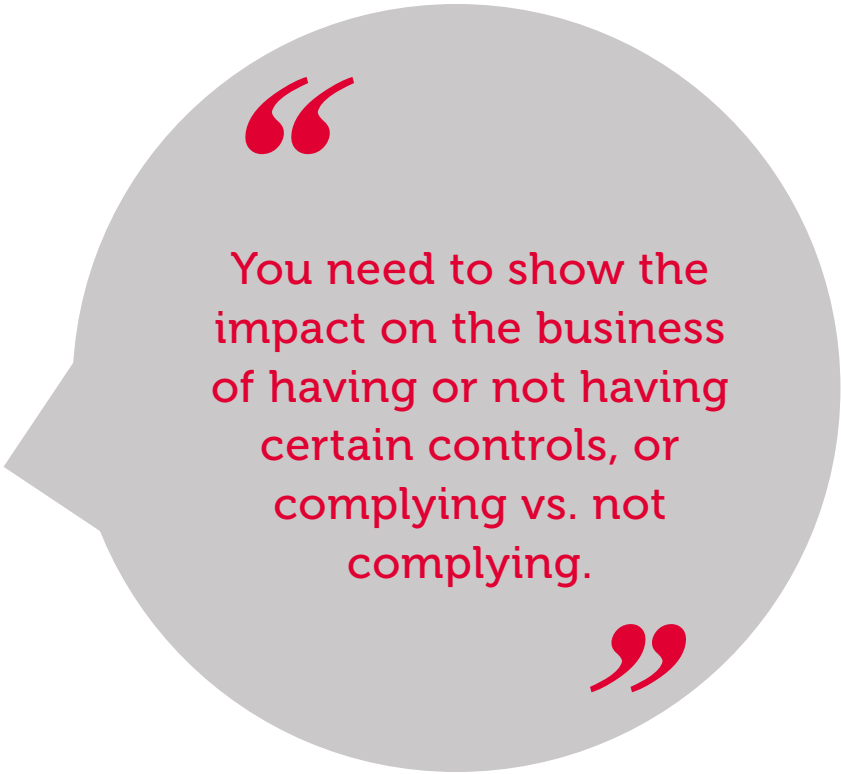
Once you have an understanding of the business and its technical assets, you need to develop an understanding of the business's overall IT strategy. For example, the business may have a well-defined strategy for moving to mobile or to other technology such as the cloud. You need to have an understanding of the bigger technology picture. "Once you understand the baseline of your organization and where they are at this point," explains Palakunnath Kunnenkeri, "then you can develop a plan to support the technical road map and how you will meet the business's security requirements." He notes that this inevitably requires prioritization. "Certain business functions will roll out very quickly, so you need to prioritize in accordance with how the business is developing," he says. Improving the maturity of a security practice means following technology changes to meet the changing needs of the business. »

> *"You have to go to the ground level and understand from the business operation what they are expecting from security."*

SECURITY MATURITY MUST BE VIEWED IN A BUSINESS CONTEXT

As technology changes, adopting new solutions needs to include evaluating the implications of those solutions in the context of both business and security strategy. For example, if the business is moving processes to the cloud, you need to understand the business advantage of doing that, but also the security implications, such as what data will reside there, the security controls you will have, and any regulatory implications. Using cloud services as an example, Palakunnath Kunnenkeri says: "Geography often defines the controls available to you. A service provider in the US may not have the same level of control in Asia. Sometimes there are regulations that have to be taken into consideration. Some of the biggest cloud providers are impacted by certain regulations, for example in Korea. Korea has one of the most stringent privacy laws." A mature security practice takes all these factors into consideration and is able to report on how well the business is protecting assets and conforming to compliance requirements.

When discussing security maturity with senior management, it is important to present security in a business context. "You can't use technical jargon," says Palakunnath Kunnenkeri. "You need to show the impact on the business of having or not having certain controls, or complying vs. not complying. Explain where the business is now and where it needs to go, and tell them the investments that are needed and resources that are required." This is the information management needs to make decisions in a business context. »



SECURITY MATURITY MUST BE VIEWED IN A BUSINESS CONTEXT

Palakunnath Kunnenkeri notes that it's important to offer senior management options, because ultimately they are the ones making the risk-based decisions. "The security strategy needs to reduce business risk. The plan has to be designed so there are multiple options to the business. This makes it possible for senior management to make the required risk-based judgements." ■

KEY POINTS

1. A mature security practice takes many operational factors into consideration as it reports how well the business is protecting assets and conforming to compliance requirements.
2. When discussing security maturity with senior management, it is important to present security in a business context.

BEGIN BY GETTING THE MOST OUT OF YOUR CURRENT INVESTMENT

DILIP PANJWANI

Chief Information Security Officer & IT Controller
Larsen & Toubro Infotech Ltd (LTI)

Dilip Panjwani is the CISO and IT controller at Larsen & Toubro Infotech Ltd. Previously, he was the director of information security at FIS Global and associate vice president and head of information-security services and ATM management at DBS Bank, India. He was included in the list of Top 100 CISOs by CISO Platform and as one of the InfoSec Maestros by InfoSecurity group. He is also a member of various thought-leadership forums involving select CISOs and CIOs.

Twitter I Website I LinkedIn

To cost effectively serve a business's security requirements, a mature security practice must have the skills and resources to get the most out of its security investment. How do you know if your security practice is really doing it's job? Dilip Panjwani, chief information security officer (CISO) and IT controller at Larsen & Toubro Infotech (LTI), says that to answer that question, you must evaluate everything you are currently doing. "You need to understand the organizational structure of the business and the various solutions that are currently deployed," he explains. "And then you need to take stock of the threat environment for this kind of organization, and look at that against the tools that are deployed and if they are effectively deployed or not. That will give a current-state assessment of the organization's maturity on security. You need to remember - One size does not fit all"

Assessing the current state of your security maturity involves really digging into your organization's investment in people, processes and technology. This includes how many security professionals you have, their backgrounds, and what exactly they do. It requires evaluating the processes and security controls you have in place, and if the company is managing to a framework or set of compliance requirements. And of course you need to look at the security technologies you have in place, if they are up-to date, and if they are actually being used. With this understanding of your current program, you can then determine if it is meeting your organization's needs today, and if it will meet them in the future, given the organization's business strategy and risk tolerance. This evaluation helps you identify your strengths and weaknesses, and it opens a dialog with other business leaders about investments needed to meet acceptable risk levels. »

> *"When you look at your current investments, you need to be sure you are getting the most out of those things."*

Assessing your current maturity in this way will also give you a good idea of what you need to do to strengthen your security program and build a more mature approach to security. Sometimes this involves investing in new technology, and sometimes it involves using the tools you have more effectively. "When you look at your current investments in technology and security, you need to be sure you are getting the most out of those things," Panjwani advises. "You need to see if configuration changes and additional training will meet the organization's needs and raise the maturity of your practice to an acceptable level." There are a couple of reasons for this. One is that you don't want to make unnecessary technology investments. The other is the practical reality of what's involved in evaluating new solutions. "An evaluation process, from the initial stack assessment through the proof of concept to the point where you are ready to implement, typically takes three to eight months," says Panjwani. "While you go through this process and get buy-in from management, you still have to have your existing stacks to avoid any breaches in the organization."

Once you have a stable security environment and you have optimized your current stack, then you need to look at what you can bring to the security stack that will reduce the operations overload on your existing teams, manage the organization attacks that are coming in, and reduce the risk level of the company. Only then will you be in a position to start addressing specific risks. "That's when you will be able to look at what are issues specifically needed to meet the risks applicable to the organization, those risks specific to your organization that you really want to address." »

> "The security team is supposed to keep the stakeholders honest in their approach."

BEGIN BY GETTING THE MOST OUT OF YOUR CURRENT INVESTMENT

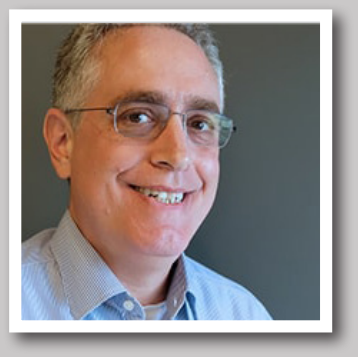
An important part of advancing the maturity of the program is communicating effectively with business leadership. "Metrics have to be defined for the organization," Panjwani says. "The security team is supposed to keep the stakeholders honest in their approach, and guide the stakeholders to help them define an acceptable risk level for the organization." ■

KEY POINTS

1. Assessing your current maturity gives you an idea of what you need to do to build a more mature approach to security. Sometimes this involves investing in new tools, and sometimes it involves using the ones you have more effectively.

2. Once you have a stable security environment and you have optimized your current stack, then you need to look at what you can bring to the security stack that will reduce the operations overload on your existing teams.

SECURITY MATURITY BEGINS AT DEPLOYMENT



JONATHAN LEVINE

Chief Technology Officer,
Chief Information Officer,
Chief Information
Security Officer
Intermedia

As CTO, CIO, and CISO at Intermedia, Jonathan Levine manages and directs 200 matrixed staff members. He has more than 20 years of experience guiding technology operations through financial, operational, and key decision-making by identifying, quantifying, and managing risks and opportunities for organizations and clients. He leads all aspects of solutions delivery for significant global initiatives, from initial conception through delivery.

Determining where your security maturity is and where it needs to be is a continuous process. "We benchmark ourselves against other companies our size and with our revenue profile, looking at how much they spend on security and how many security engineers they have, and issues that other companies like us have had," says Jonathan Levine, chief technology officer, chief information officer, and chief information security officer (CTO/CIO/CISO) at Intermedia. "We also meet cross-functionally with executive leaders once a quarter. At the beginning of the year, we have a register of things we plan to do during the year. We go over things that are endangering our security posture and how we plan to resolve them." As they go through the year, they compare the things they said they would improve to what they actually accomplished, and in that way they can see their progress. This can include activities such as tracking progress through the year, taking account of unforeseen threats that could disrupt their original plan, and reporting progress to executive teams and building the case for investing in necessary tools and resources.

Levine recommends several practices that can improve the overall security maturity within an organization. He says one of the best places to start is the development pipeline. "The first question to ask is how do your applications get into production? Is it automated, or are there manual steps involved?" He points out that with a manual process, it is difficult to tell the difference between a developer who's working through valid steps in real deployment work and a bad actor planting malicious code. "If you push your deployment and release pipeline into an automated process, then it's much easier to tell the difference between changes made in production that are legitimate versus »

> *"We meet cross-functionally with executive leaders once a quarter. We go over things that are endangering our security posture and how we plan to resolve them."*

ones that are not," Levine explains. A greater focus on the development pipeline underscores the role developers play in the overall security strategy, and it can save you time and resources in securing applications once they're in production.

Another strategy involves restricting what you can do with production machines. Levine says, "In the world of containers and virtual machines, you can restrict one machine to one function, and then you can harden that machine's access to outside resources." For instance if you have a manual server, that machine should not be contacting outside web servers. Taking that a step further, you can build these kinds of rules into an automated development and deployment pipeline. "If you can combine outbound networking rules with your automated deployment strategy, then you can make it so any of these machines that could be compromised are less likely to be able to do anything if they are compromised," he points out.

Improving security maturity often requires investing in new security technologies or replacing outdated ones, but Levine notes the importance of doing this thoughtfully. "The number-one worst reason for buying new security technology is that it's November and you've got money left in the budget," he says. One approach to buying a new technology is you have a process that works but it's human-intensive and you're looking to make it more efficient. For example, if your SIEM operators say they spend most of their day chasing alerts, you might look for a technology solution to take that off their plates so they can focus on more serious issues. Another approach to »

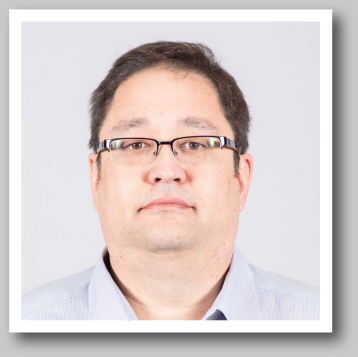
> "The number-one worst reason for buying a new security tool is that it's November and you've got money left in the budget."

investing in technology is to address a more speculative need. A vendor tells you of a threat you should be addressing and promotes a tool to address it, or one of the board members mentions a new technology to your CEO. It's important to be always open to new technologies and ways to improve security maturity, but is that a threat you really need to worry about, and is the vendor's tool the best solution? "In those cases, start slowly to prove the concept with real metrics," says Levine. "Measure to see if you are really experiencing that kind of threat, and then try the solution on a few systems to see if it makes a difference." ■

KEY POINTS

1. Determining where your security maturity is and where it needs to be is a continuous process.
2. When investing in new security tools, make sure the challenge that solution is addressing is one faced by your organization and that it maps to priorities you and your cross-functional team identified as important to your business.

THE SECURITY MATURITY DISCUSSION SHOULD BE RISK-BASED



LESTER GODSEY

Chief Information Security Officer
City of Mesa, Arizona

Lester Godsey is the CISO for the City of Mesa, Arizona. With over 24 years of public-sector IT experience, Godsey has presented at the local, state, and national levels on topics ranging from telecommunications to project management to cybersecurity. He has taught technology and project management at the collegiate level. A published author, he holds a BA in Music and an MS in Technology from Arizona State University.

LinkedIn

Before you can measure the maturity of your security practice, you must understand what your security strategy involves, and you must understand its business context. Lester Godsey, chief information security officer (CISO) for the City of Mesa, describes this as getting the lay of the land. "A CISO can't just focus on cybersecurity and the technical aspects of that role. The CISO needs to understand the enterprise's products and services from the business perspective as well as the cybersecurity perspective."

This involves having some kind of framework or security scorecard you can use with other executives and managers in the organization, and based on their feedback, develop common understanding of risk sensitivities and priorities in different areas of the business. "I report to the chief information officer [CIO]," Godsey explains. "I have a simple weighted-scorecard approach for measuring risk that I use to show my CIO where our priorities are. Organizations are fluid entities, and their priorities are always changing. I have a process in place where I constantly ask and adjust as needed, based on feedback from business managers. My CIO and my senior management appreciates that. It builds the relationship, and it gives me the ability to have more autonomy in making decisions, because all my decisions are based on those risk prioritizations."

Godsey makes risk a key measurement in assessing security maturity, but there are other factors too, including alignment with organizational strategy and cost to the organization. Regardless of the scoring method you use, it's important to have a repeatable methodology so you can have intelligent »

> *"The CISO needs to understand the enterprise's products and services from the business perspective as well as the cybersecurity perspective."*

discussions about where you stand and what you need to do. He says, "You have to have a baseline understanding of what's important to the organization so that you can subsequently say, 'We're at this level of maturity within this area as opposed to this other level in a different area.'"

Those kinds of discussions are the basis for a considered approach to security investments. Godsey says too many organizations make strategic decisions based on the latest incident or a report promoting some new technology as the path to greater security maturity. These approaches may win spending approvals in the short term, but there's a downside. "It's like crying wolf. It may work for the first or second time, but if your CISO's doing that to drive the cybersecurity program, eventually it's going lose its effect."

A mature security practice needs to tie back to the mission and vision of the organization. It has to consider the current risks to the organization and how to address them. "Those are the drivers that make more sense when having an intelligent conversation with your management about the maturity of your security practice," says Godsey. There needs to be a methodical way of identifying the security needs of the organization in terms of business risk, cost, and strategic alignment. ■

> "I have a simple weighted scorecard approach for measuring risk that I use to show my CIO where our priorities are."

KEY POINTS

1. Risk is a key measurement in assessing security maturity, but there are other factors too, including alignment with organizational strategy and cost to the organization.
2. A mature security practice needs to tie back to the mission and vision of the organization. It has to consider the current risks to the organization and how to address them.

XAVIER MERTENS

SANS ISC, Senior Handler
Xavier Mertens Consulting,
Freelance Security
Consultant & Owner

Twitter I Blog I Website

A key factor is to know the business so that you can prioritize projects that quickly improve the overall security posture. I suggest a new CISO should work closely with the management to understand the business and get their approval for new projects. Often a good starting point when you have a limited budget and staff is to enforce best practices.


Mature Your Security & Risk Program
Work with Trustwave to plan, build and execute an optimized security program.
• Understand your risks and how to mitigate them.
• Optimize your current investments.
• Augment your team.
Learn More
Trustwave®